Lo que la evidencia esconde.

METODOLOGÍA DE ANÁLISIS FORENSE ESTANDARIZADA PARA DISTINTOS ESCENARIOS

Pilar Vila Avendaño | Forensic & Security



Forensic & Security

Sobre mi...

Pilar Vila Avendaño

Analista Forense Digital

CEO & COFUNDADORA

DFTools y Forensic&Security

- ✓ Certificado CHFI (Computer Hacking Forensic Investigator).
- ✓ Ingeniera informática & Consultora y Perito Forense Informático.
- ✓ Profesora, formadora y autora del libro “Forensic Analysis Techniques for Computer Forensics Expert Witness” de 0xWord.

pilar.vila@forensic-security.com

@PilarinaVilla

linkedin.com/in/pilar-vila-forensicsec/

SO IT BEGINS

memegenerator.net



Empecemos por lo que no es





KEEP CALM AND LET KARMA FINISH IT

Actividad del perito

Evidencias y técnica

Evidencias Digitales

Informática Forense

Contextualización

Situación y contexto

Pericial Informática

Resumen de la actividad del perito informático

Informe y/o Ratificación

Demostración



EVIDENCIA DIGITAL



- En la actualidad vivimos en un mundo digital globalizado en donde IoT, smartphones, servidores y equipos informáticos personales pueden ser víctimas de los más diversos ataques cibernéticos cuyo objetivo son:

negocios, personas o instituciones



El conjunto de datos o información en formato binario, como por ejemplo ficheros, su contenido o referencias a éstos (metadatos), capturas de tráfico o conexiones de red, imágenes de discos o tarjetas, o memoria volátil del sistema atacado, entre otros, que puedan ser utilizados para esclarecer un hecho o un incidente de seguridad.



Todo lo que pueda almacenar información de forma física o lógica que logre ayudar a esclarecer un caso



CONCEPTOS FUNDAMENTALES

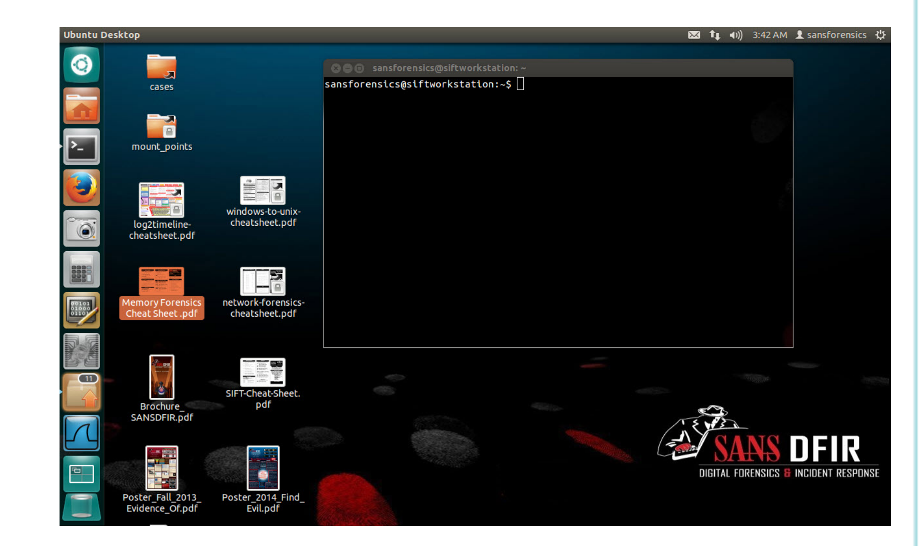


SIFT Workstation

Es una distribución forense informática basada en Ubuntu.

Incluye todas las herramientas necesarias para realizar un examen detallado de Incident Response y análisis forense digital.

- Este kit tiene la capacidad de examinar de forma segura discos sin formato, sistemas de archivos múltiples, etc.
- Establece pautas estrictas sobre como se examinan las pruebas (solo lectura) y verifica que las pruebas no sufran modificaciones.





Kali

Es una distribución basada en Debian GNU.

Está especialmente dirigida a la auditoria y seguridad informática en general.

- Trae mas de 600 programas como Nmap, Wireshark, John the Ripper y Aircrack-ng.
- Puede ser usado en su versión Live o instalada como Main-OS.
- Dispone de las herramientas forenses de software libre mas populares de forma rápida y sencilla.







Santoku

Es una distribución forense basada en Lubuntu y diseñada para la auditoria y análisis de dispositivos móviles.

Incluye:

- Herramientas para desarrollo para Android.
- Herramientas de pentesting.
- Herramientas de análisis forense especializado en smartphones.





Distribuciones:

CAINE Linux



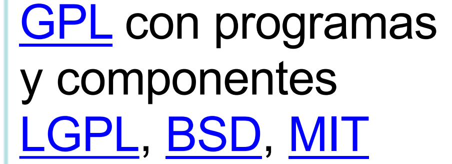
CAINE es el acrónimo de Computer Aided Investigate Enviroment.

Ofrece un entorno integrado con las herramientas de software forense existentes y una interfaz grafica amigable.

Sus principales características son:

- Un Entorno fácil que apoye las investigaciones digitales.
- Una Interfaz gráfica amigable.
- Herramientas amigables para el usuario.

CAINE representa plenamente el espíritu de la filosofía Open Source, ya que el proyecto está completamente abierto y todo el mundo puede asumir el legado del desarrollador anterior o gerente del proyecto.


GPL con programas y componentes LGPL, BSD, MIT



1. **Si se encuentra encendido no se debe apagar**, ya que se perderían todos los datos volátiles como por ejemplo procesos activos, y todo lo que esté cargando en la memoria RAM.
2. **Cuando el dispositivo se encuentre apagado no debe encenderse**, debido a que al cargarse nuevamente el sistema podría sobrescribir información útil e inclusive podría tener algún código malicioso que destruya las evidencias de forma automática, borrando así las huellas del incidente.



Relevante:

- La evidencia es preciso que este relacionada con el delito bajo investigación.
- Que haya sido obtenida en un modo adecuado. Además, debe estar correctamente identificada.
- Debe ser confiable es decir que no haya sido modificada (respetando su cadena de custodia).



La CdC establece un mecanismo o procedimiento, que asegura a quienes deben juzgar que los elementos probatorios (indicios, evidencias o pruebas) no han sufrido alteración o contaminación alguna desde su recolección, examen y custodia, hasta el momento en el cual se presentan como prueba ante el Tribunal.

Este procedimiento debe controlar dónde y cómo se ha obtenido la prueba, qué se ha hecho con ella (y cuándo), quién ha tenido acceso a la misma, dónde se encuentra ésta en todo momento y quién la tiene.

En caso de su destrucción (por la causa que sea), cómo se ha destruido, cuándo, quién, dónde y porqué se ha destruido.

Este procedimiento de control debe ser absolutamente riguroso, de manera que no pueda dudarse ni por un instante de la validez de la prueba.



1. No confiar únicamente en la información proporcionada por los programas del sistema

- Es posible que los sistemas comprometidos puedan haber sido manipulados por los atacantes o algún código malicioso.
- Esto se conoce como técnicas antiforenses.



2. No ejecutar aplicaciones que modifiquen la fecha y hora de acceso de los archivos del sistema

- Estudiar el TimeLine es una de las técnicas de análisis forense más potentes para entender el paso a paso de los incidentes.
- Realizando una línea temporal basada en los tiempos MAC (Modificado, Accedido, Cambiado) de cada fichero y correlacionando distintos logs, puede identificarse el cómo y cuando de muchos hechos o incidentes.
- Ejecutar aplicaciones que cambien los metadatos de los archivos sería un error muy grave



3. Utilizar técnicas de clonado que no alteren la evidencia

- Es fundamental aplicar técnicas forense que garanticen la prueba



Clonado:

```
root@kali:~# mount -o rw /dev/sde1 ./disco2
root@kali:~# dc3dd if=/dev/sda of=./disco1/[redacted].dd log=./disco1/[redacted].log verb=on hash=sha1 hash=sha512

dc3dd 7.1.614 started at 2015-01-13 12:25:07 +0000
compiled options:
command line: dc3dd if=/dev/sda of=./disco1/[redacted].dd log=./disco1/[redacted].log verb=on hash=sha1 hash=sha512
device size: 312500000 sectors (probed)
sector size: 512 bytes (probed)
160000000000 bytes (149 G) copied (100%), 2796.2 s, 55 M/s

input results for device `/dev/sda':
   312500000 sectors in
   0 bad sectors replaced by zeros
   358[redacted]277b971f0d930a3c2c9531be3e (sha1)
   c2a[redacted]e604df6df8f7b28c8cf35033e7a95fb2d7c59851f99b15290c15e92125bcfe591ecd02c5149dc37e1462cbccca321e89 (sha512)

output results for file `./disco1/[redacted]dd':
   312500000 sectors out

dc3dd completed at 2015-01-13 13:11:44 +0000
```




Tipos de casos

- Competencia desleal y fuga de información
- Estudio de software: incumplimiento de contrato, plagio, propiedad intelectual…
- Correos electrónicos y WhatsApp en acoso, estafa, etc.
- Valor probatorio de una dirección IP
- Grabaciones en soportes digitales
- Periciales no forenses



GUÍAS



- Norma ISO/IEC 27037:2012 “*Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*”
- guía de cómo llevar a cabo la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, y en su capítulo 7 trata la cuestión de la CdC en este ámbito.
- Esta norma viene a sustituir a las antiguas directrices RFC 3227, norma más dirigida a dispositivos actuales y más acorde con el estado de la técnica actual.



- **Familia UNE 71505:2013 (71505-1, 71505-2, 71505-3)**
- **UNE 71506:2013. Proceso de análisis forense**
- **UNE 197010:2015. Criterios sobre elaboración de informes**

Especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba AENOR, organismo reconocido a nivel nacional e internacional por su actividad normativa (Ley 21/1992, de 16 de julio, de Industria).



- **RFC 3227. Recolección y manejo de evidencias**
- **RFC 4810. Preservación de la información**
- **RFC 4998. Preservación de la información incluída la firmada digitalmente**
- **RFC 6283. Demostración de la integridad y validez de la información**

Serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de internet y otras redes.



- **ISO/IEC 27037:2012**

Norma para la recopilación de evidencias

- **ISO/IEC 27042:2015**

Norma para el análisis y la interpretación de la evidencia digital



- Que norma debo aplicar?



The Sleuth Kit

TSK es una recopilación de herramientas para realizar análisis forenses.

Se puede usar para examinar la mayoría de versiones de Windows, macOS, Linux y equipos con UNIX.

Se puede usar vía CLI o como una librería embebida en una herramienta forense aparte, como puede ser Autopsy.



IBM Public License, CPL, GPL 2

Autopsy

Autopsy proporciona una interfaz grafica para The Sleuth Kit.

Dispone de una versión de escritorio muy completa en Windows y una interfaz web para Linux.

Esta herramienta se diseño bajo los siguientes principios.

- Extensible.
- Centralizado.
- Fácil de usar.
- Multiusuario.



GPL2, Apache 2



LiME

LiME, anteriormente DMD, es un Loadable Kernel Module (LKM) que permite la adquisición de la memoria volátil en Linux y dispositivos basados en Linux (Android).

Esta herramienta permite adquisición de memoria directamente al sistema de archivos del dispositivo o a través de la red.

Es la primera herramienta que permite hacer capturas completas de memoria de dispositivos Android.

```
include(dirname(__FILE__) . '/bootstrap/unit.php'); // Include lime.

// Create the lime_test object for 10 number of assertions and color output.
$t = new lime_test(10, new lime_output_color());

// The test array.
$arr = array('Hello', 'World', 123,);

// Output a comment.
$t->diag('in_array()');

// Test to make sure in_array returns a boolean value for both values
// that are in the array and not in the array.
$t->isa_ok(in_array('hey', $arr), 'bool', '\'in_array\' did not return a boolean value.');
$t->isa_ok(in_array('Hello', $arr), 'bool', '\'in_array\' did not return a boolean value.');
$t->isa_ok(in_array(5, $arr), 'bool', '\'in_array\' did not return a boolean value.');
$t->isa_ok(in_array(FALSE, $arr), 'bool', '\'in_array\' did not return a boolean value.');

// Test to make sure in_array can find values that are in the array
// and doesn't find values that are not in the array.
$t->ok(!in_array('hey', $arr), '\'in_array\' found a value not in the array.');
$t->ok(!in_array(5, $arr), '\'in_array\' found a value not in the array.');
$t->ok(!in_array(FALSE, $arr), '\'in_array\' found a value not in the array.');
$t->ok(in_array('Hello', $arr), '\'in_array\' failed to find a value that was in the array.');
$t->ok(in_array('World', $arr), '\'in_array\' failed to find a value that was in the array.');
$t->ok(in_array(123, $arr), '\'in_array\' failed to find a value that was in the array.');
```




Volatility

Volatility es un framework forense Open-Source para respuesta ante incidentes y el análisis de malware.

Esta escrito en Python y es compatible con Windows, MacOS X y sistemas Linux.

Contiene múltiples herramientas, también escritas en Python.

Permite analizar volcados de memoria RAM de 32 y 64 bits.





Ejemplos claros de los campos donde no existe una metodología de estudio son:



La Industria 4.0 supone un reto para el analista forense ya que no existen ni metodologías ni herramientas de estudio.



Actualmente se hacen estudios de un número limitado de dispositivos, no existen mecanismos forenses que permitan volcar grandes cantidades de información para estudiarla posteriormente en conjunto.



Existe muy poco software que permita hacer un análisis forense de datos en una nube, ya sea pública o privada.



Está empezando a salir al mercado software forense para el estudio de drones pero, tiene un coste muy alto o bien es muy específico.

Por ejemplo, existe un framework concreto del que se habla en "Drone forensic framework: Sensor and data identification and verification" con ISBN: 978-1-5090-3202-0, publicado en 2017.



Cuando se produce un ciberataque no se hace un estudio in situ del mismo, siempre se hace el estudio a posteriori, una vez solucionado, y muchas veces es *post mortem*, es decir, con equipos apagados y una vez alterados.



Sin procesado intermedio:

Ante incidentes de ciberseguridad, los sistemas software actuales normalmente no aportan tramas de red en crudo, sin procesar, por lo que el experto no puede estudiar las tramas sin modificaciones. Los sistemas como los IDS (Intrusion Detection System o sistema de detección de intrusión), los IPS (Intrusion Prevention System o sistema de prevención de intrusión) y los SIEM (Security Information and Event Management o información de seguridad y gestión de eventos), aportan un filtrado de la información sobre el que se ha aplicado un estudio previo.

Sin embargo, para el experto, el poder detectar patrones o información relevante en las situaciones críticas, que pasan desapercibidos para determinado software puede ser crítico.



Tendrá un rol importante en el desarrollo de herramientas forenses.



EL NOTARIO



¿Quien me garantiza la veracidad de lo que estoy viendo?

¿Que puedo hacer?





LA LEY



Veracidad y certificación





Thriller basado en hechos reales
:(
Your PC ran int
rt for
you.
his error: SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (
Microsoft Warns
Use Windows 7
'At Your Own Risk'
Internet Explorer
This page has an unspecified potential security risk.
Would you like to continue?
Yes
No
Warning!
Spyware detected on your computer!
Install an antivirus or spyware remover to clean your computer
Danger!
Danger!
Warning! Win32/Adware.Virtumonde
Detected on your computer
Warning! Win32/PrivacyRemover.M64
Detected on your computer
Please activate your antivirus software to Clean your computer

Forensic & Security



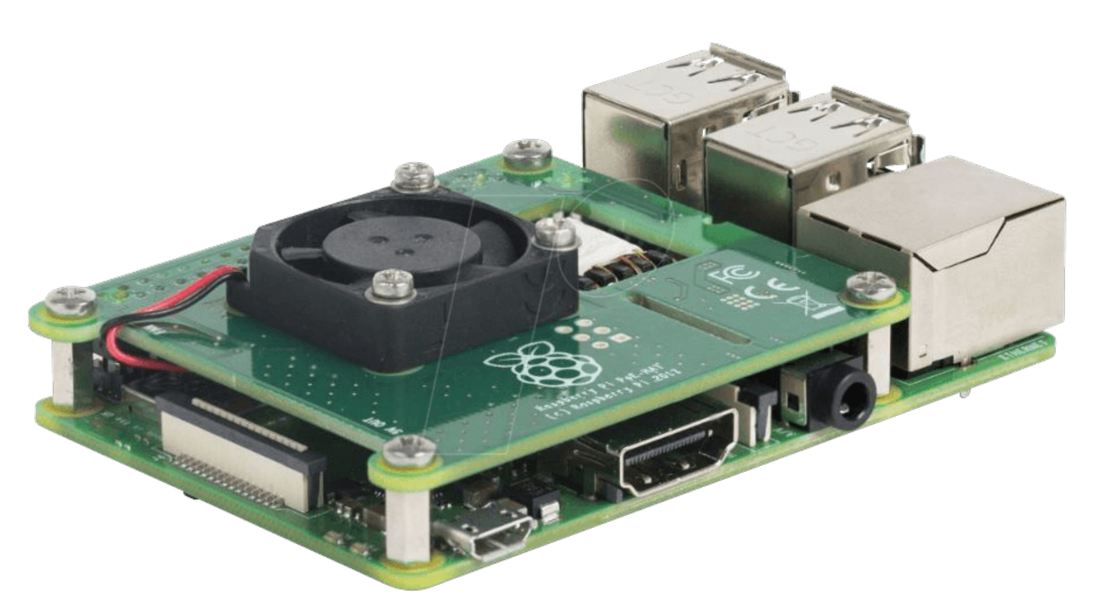
EL PLAGIO



En este caso, se estaba valorando el plagio de una app de Android.

Utilizamos cURL para recuperar el .apk y APKTool y DEX2JAR para poder analizar el código de las dos aplicaciones.

Se utiliza un plugin de comparación en Notepad++ para determinar si la aplicación había sido plagiada.





cURL://

cURL es un proyecto software que provee de una librería (libcurl) y una herramienta de línea de comandos (curl) para realizar transferencia de datos a través de distintos protocolos.





$ curl http://es.wikipedia.org

APKtool

Es una herramienta que permite realizar ingeniería inversa a apps de Android.

Puede decodificar recursos hasta su forma original y reconstruirlos después de haber realizado alguna modificación.

```
$ apktool d test.apk
I: Using Apktool 2.4.0 on test.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: 1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
$ apktool b test
I: Using Apktool 2.4.0 on test
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

Apache 2.0



DEX2JAR

La mayoría de las aplicaciones para Android están programadas en Java, los instaladores de estas, tienen una extensión ".APK", que no es mas que una variación de la extensión ".JAR". Ambos archivos se pueden abrir con cualquier compresor de archivos.

Dentro de ellas, encontraremos archivos ".DEX". Estos ficheros se pueden convertir a formato ".JAR" utilizando la herramienta Dex2Jar.

```
root@kali:~# d2j-jar2dex -h
d2j-jar2dex -- Convert jar to dex by invoking dx.
usage: d2j-jar2dex [options] <dir>
options:
 -f,--force                   force overwrite
 -h,--help                    Print this help message
 -o,--output <out-dex-file>   output .dex file, default is $current_dir/[jar-name]-jar2dex.dex
version: 0.0.9.15
```



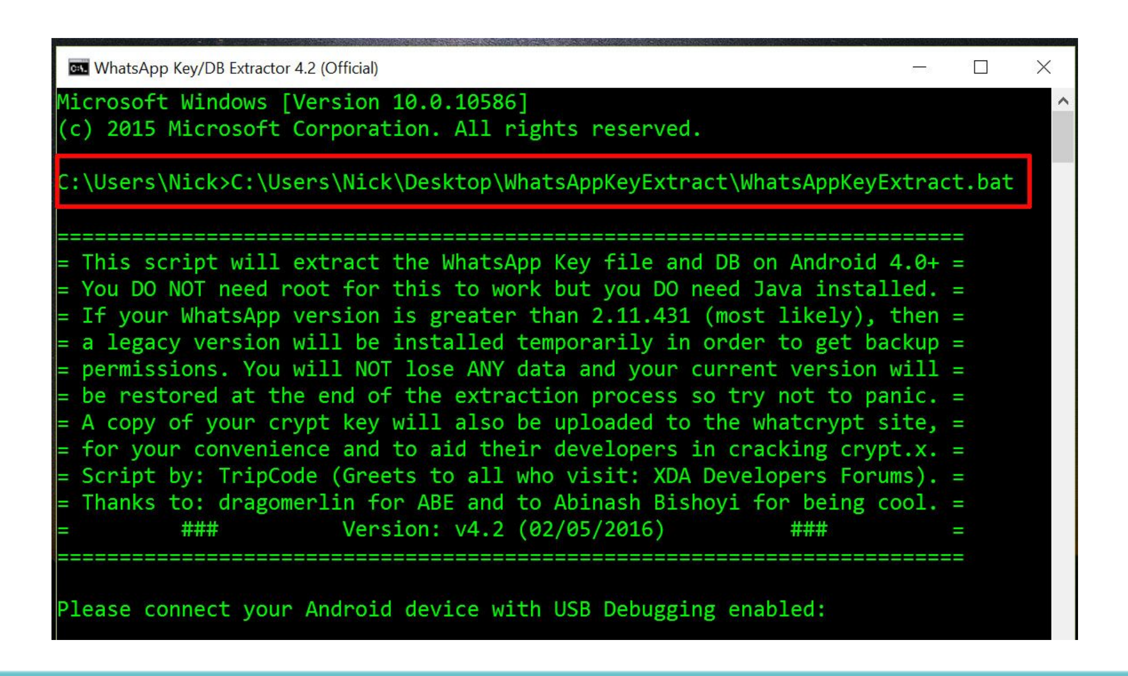

Móviles chinos



Recibimos un móvil de una marca china, con la excusa de que hacia “cosas raras”.

Inicialmente dudamos del caso, finalmente lo aceptamos y se realiza un backup del dispositivo con ADB y continuamos el análisis.

Procedemos a analizar la BBDD de WhatsApp y para ello utilizamos WhatsApp Key DB Extractor para recuperar la clave de cifrado de la misma.



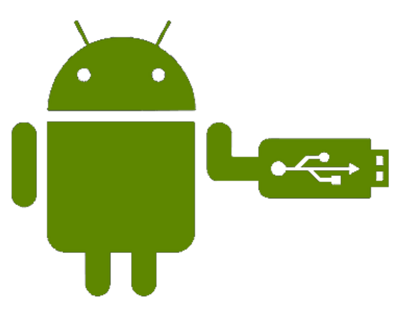


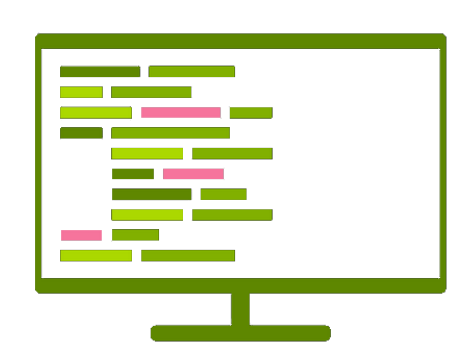
Android Debug Bridge

Es una herramienta de línea de comandos versátil que permite comunicarse con un dispositivo Android.

Consta de tres partes principales:

- Cliente: Envía los comandos.
- Daemon: Ejecuta los comandos en el dispositivo.
- Servidor: Administra la comunicación entre cliente y Daemon.

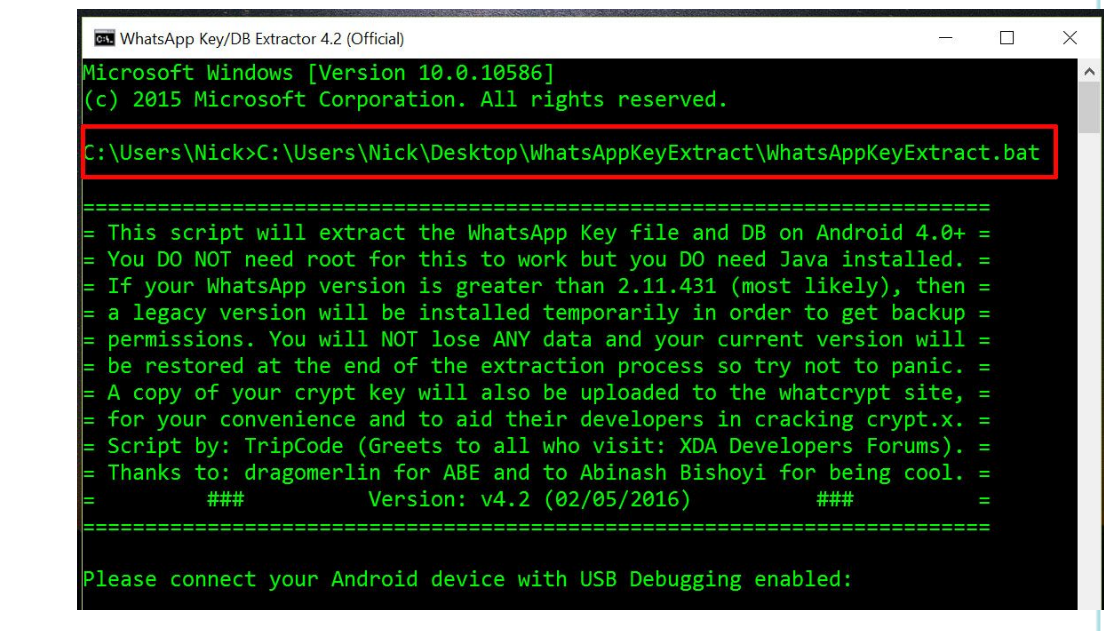




WhatsApp Key DB Extractor

Todas las bases de datos correspondientes a los mensajes enviados por WhatsApp se encuentran en el almacenamiento interno del dispositivo en el que tengamos configurada la cuenta.

Para poder hacer un análisis sobre una BBDD cifrada, se utiliza WhatsApp Key DB Extractor.





Una vez realizamos el backup y desencriptamos la BBDD de WhatsApp, nos damos cuenta de que el teléfono está rooteado.

No solo eso, sino que las aplicaciones instaladas en el dispositivo provenían de Aptoide y estaban llenando de malware el dispositivo.

Sin embargo, procedemos a realizar un esnifado de red para ver que es lo que estaba pasando. Para ello, creamos una zona WiFi con una Raspberry Pi.

Los resultados determinaron que el teléfono estaba mandado datos privados a servidores en China.





JUGANDO VOY



Un grupo de menores estaban siendo acosados por uno de los administradores de un servidor del juego.

De este caso, solo teníamos constancia de un un correo electrónico y un nickname.

Gracias al uso de herramientas OSINT se pudo localizar una IP que pudo llevar al acosador.



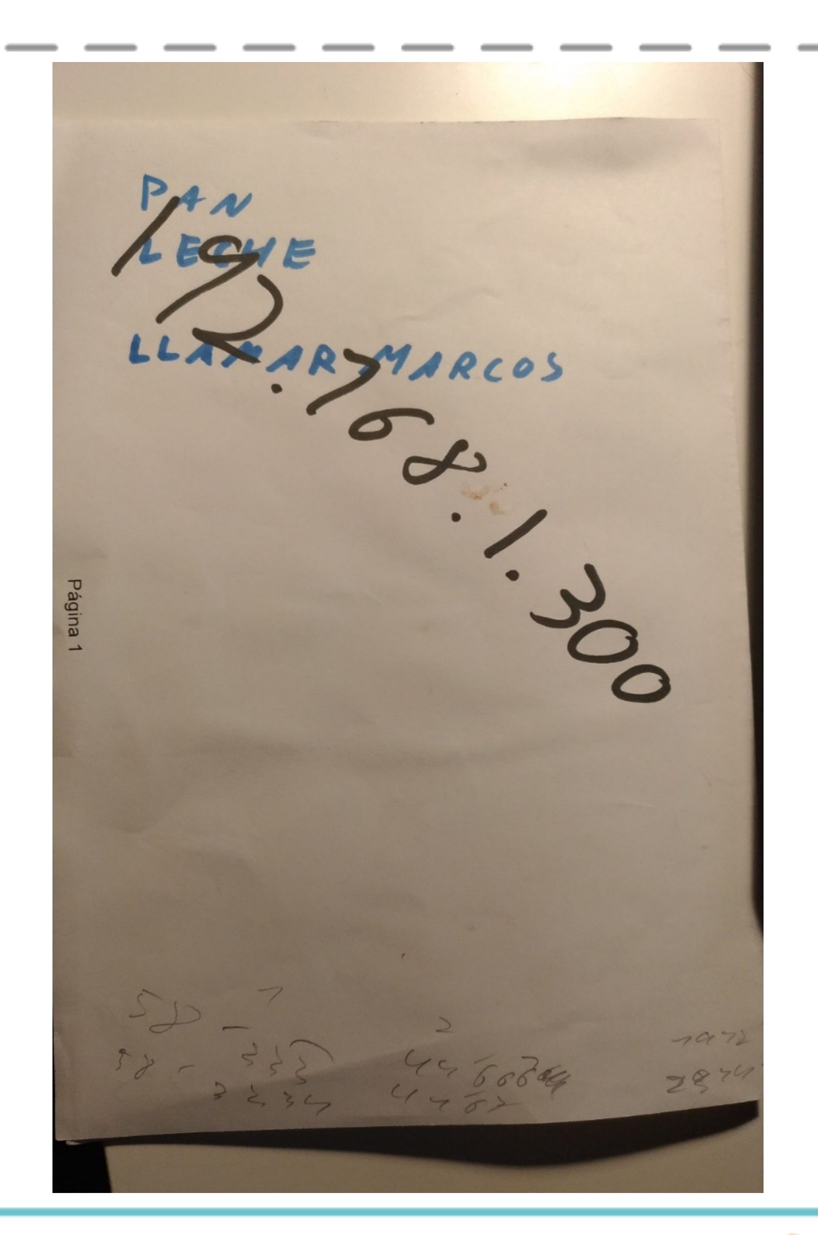


EL VALOR DE UNA IP



Cual es mi IP

- Una Ip en una fotocopia: 5 años de cárcel por robar 3000€
- Buscar toda la información pertinente de la época
- Explícalo todo y convéncelos
- Reconstrucción aproximada de la fotocopia, la original estaba peor:





LAS CAPTURAS DE PANTALLA



Cual es mi identidad

- 2 años de cárcel: A Laura y a Lucía les gusta el origami
- Lucía no era buena gente
- To be continued…





AL MARGEN DE LA LEY



- No me mandes más correos





FUGAS



Solemos encontrar casos en que uno o varios empleados estaban filtrando información confidencial de la empresa.

Gracias a la cantidad de ficheros adjuntos que se encontraban en esa serie de correos, se realiza un análisis de metadatos con ExifTool, que nos permitió verificar que el creador de dichos documentos era en efecto el dueño de la empresa.



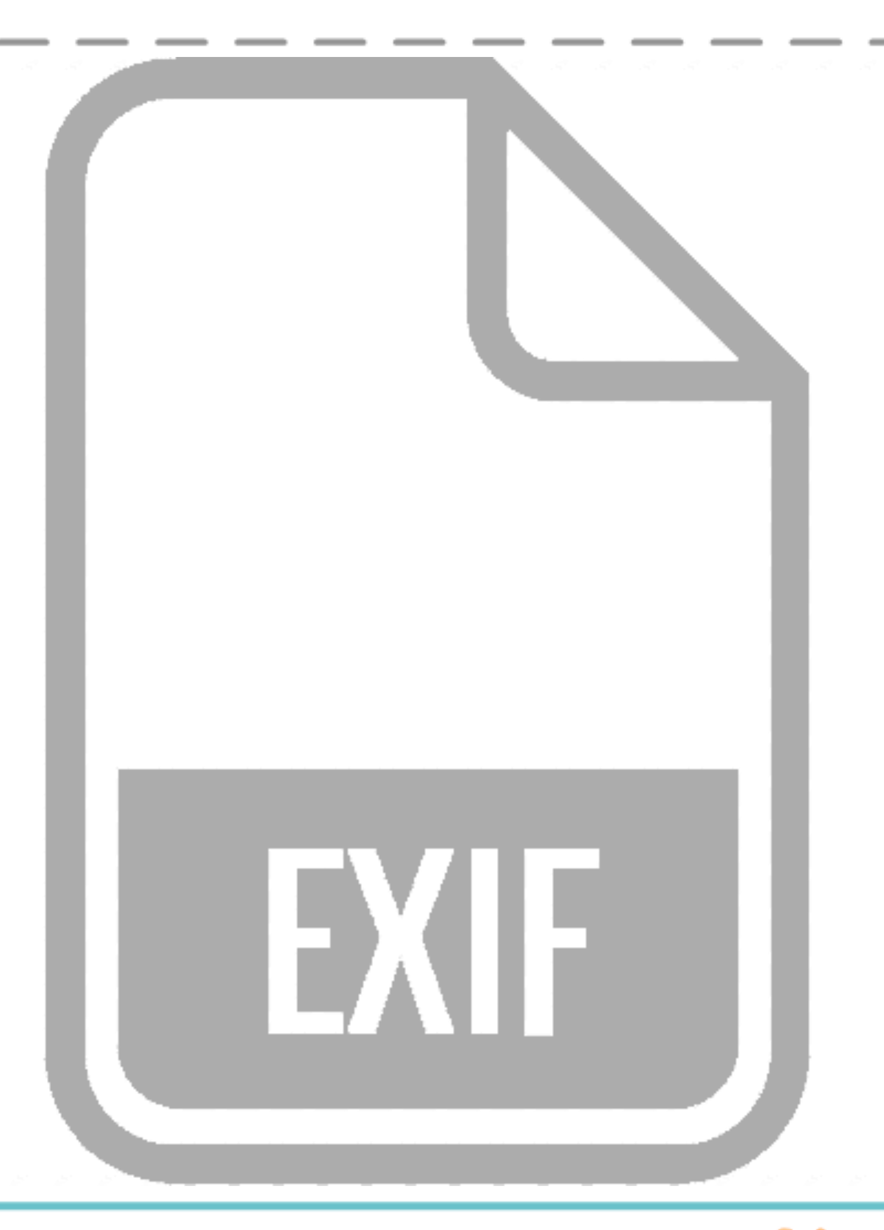


EXIF Tools

Es un software para leer metadatos de imágenes, audio, video, PDF, etc.

Esta disponible como una librería de Perl como una aplicación CLI.

Flickr utiliza ExifTool para parsear los metadatos de las imágenes subidas.



En Linux, dentro del directorio /var/log del sistema, se encuentran multitud de directorios y ficheros con información muy valiosa, desde errores (para detectar y corregir problemas), mensajes generales del sistema, autenticación, registro del kernel, etc.
Otros servicios almacenan sus logs en su propio directorio, como sería el httpd.

A modo de comparación, en Windows hayamos el Visor de Eventos.
Este contiene registro de eventos de Aplicación, Seguridad, Instalación, Sistema, etc.
El visor de estos registros, permite realizar filtros, exportar los logs, y es una herramienta muy útil a la hora de subsanar problemas o investigar para saber que ha pasado en una determinada circunstancia.

Resulta vital para el SysAdmin la correcta gestión, revisión y administración de los logs. Gracias a ellos se dispone de información que de otra manera no existiría. Gracias a los logs, nos podemos preparar.

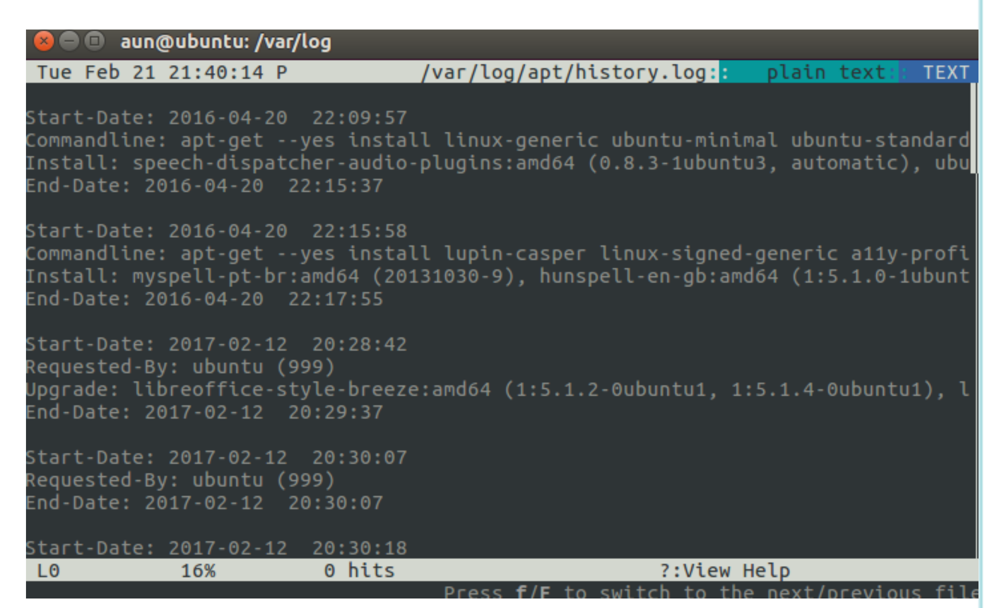




Comparación de logs



Logs en la naturaleza



Logs en Linux

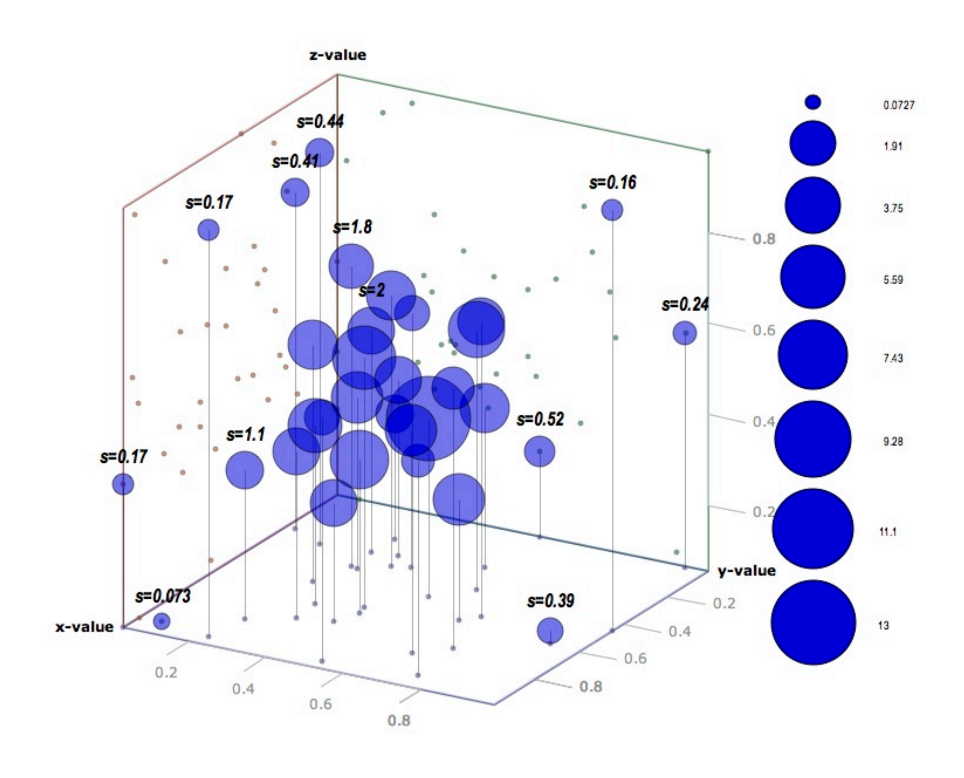


NAVEGANDO VOY



Proxy

- Debería estar trabajando
- Hace más de un año que formatearon su ordenador
- Siempre me quedará Squid proxy, Excel y Matlab



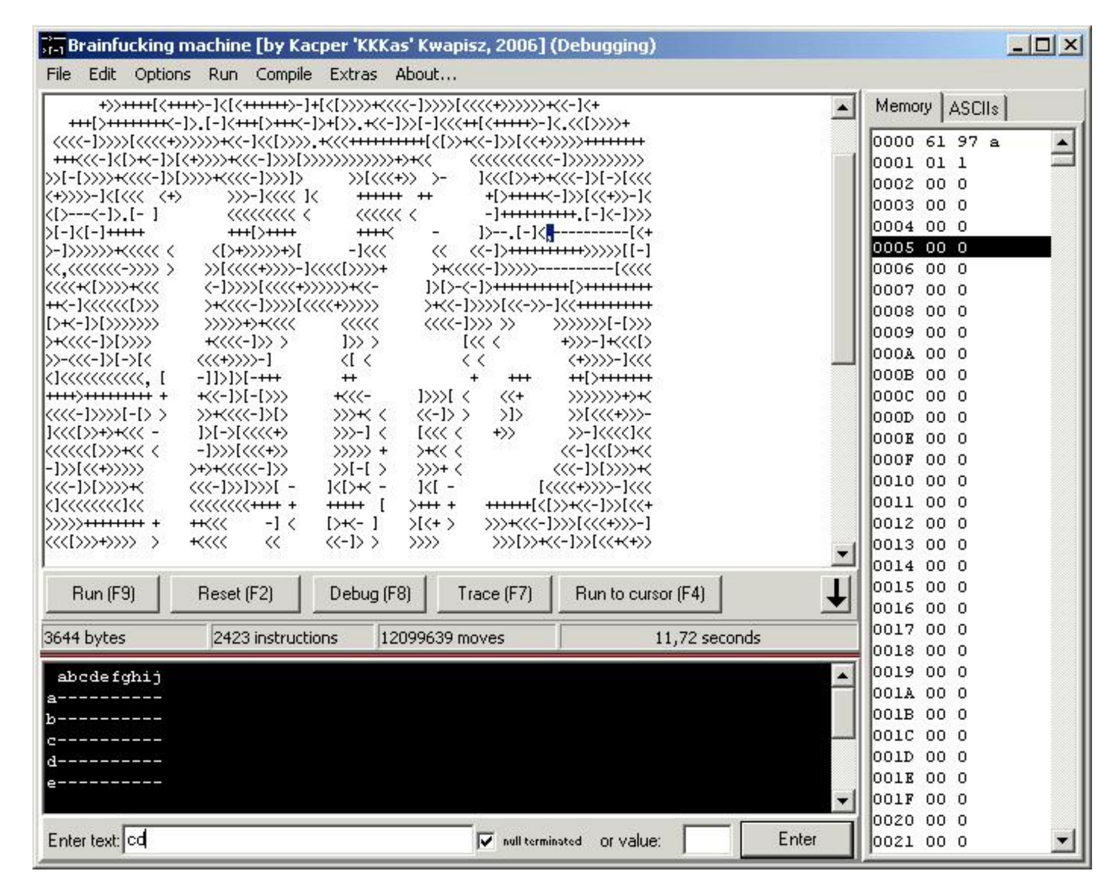




LOS 90 HAN VUELTO



- Parecía algo sencillo, verificar que una aplicación no cumplía las funcionalidades





CUANDO JOHANA LLEGÓ A MI VIDA



- Johana se llamaba Manolo





Yara

YARA es una herramienta enfocada a (pero no limitada a) ayudar a investigadores a identificar y clasificar malware, basándose en patrones binarios o textuales.

YARA es multiplataforma. Funciona en Windows, MacOS X y sistemas Linux.

Se puede usar a través de la consola de comandos o en scripts de Python con la extensión “yara-python”.

```
rule MAL_ZombieBoy_Malware_Gen_Feb19_1_RIDDC6 : EXE FILE MAL GEN {
   meta:
      description = "Detects ZombieBoy malware"
      author = "Florian Roth"
      reference = "https://www.alienvault.com/blogs/labs-research/zombieboy"
      date = "2019-02-05 15:47:31"
      score = 70
      customer = "x23"
      required_modules = "pe"
      minimum_yara = "3.0.0"

   strings:
      $x1 = "C:\\Users\\ZombieBoy\\" ascii
      $s1 = "C:\\Windows\\System32\\sys.exe" fullword ascii
      $s2 = "RookIE/1.0" fullword ascii
   condition:
      uint16 ( 0 ) == 0x5a4d and filesize < 200KB and (
         pe.imphash ( ) == "6a79728a09f4edda13797e5ae0ffa0f3" or
         1 of ( $x* ) or
         2 of them
      )
}
```




EL VALOR DE LO OCULTO



- Formateado
- Intel Rapid Storage Technology





Foremost

Es una potente herramienta que permite recuperar ficheros desde distintos sistemas de ficheros.

Permite aplicar distintos filtros que proporcionan distintos resultados:

- -w Extrae un listado de todo lo que se puede recuperar
- -t Permite recuperar un formato de archivo
- -q Activa el modo rápido

Can you get my stuff back? Today? Please?

cbldatarecovery.com/blog
CBL

Whadaya mean "BACKUP"?

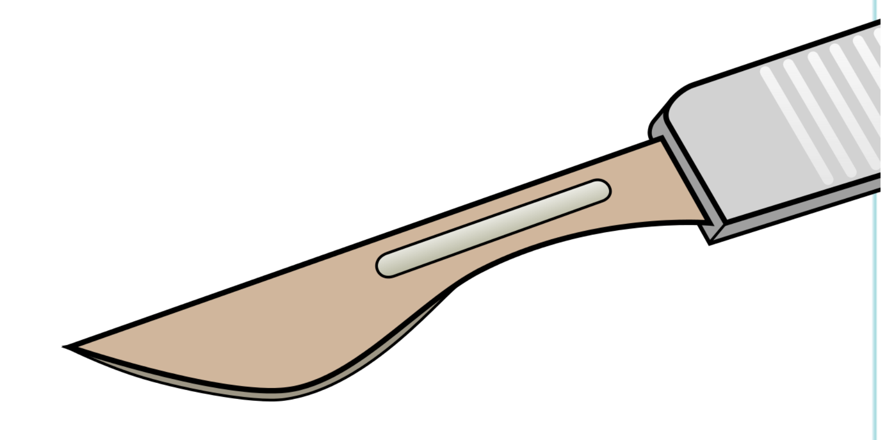


Scalpel

Permite recuperar archivos borrados.

Es una herramienta muy útil ya que permite identificar y recuperar ficheros casi al instante.

Funciona independientemente del sistema de archivos.



MI CUÑADO
““INFORMATICO””
¯_(ツ)_/¯



- Soy el administrador de una web, ¿Qué hago?
- En los foros de mi web hay discusiones demasiado acaloradas sobre Kim Jong Un y Trump
- ¿Qué hacemos?
- Volvemos a la importancia de los LOGS



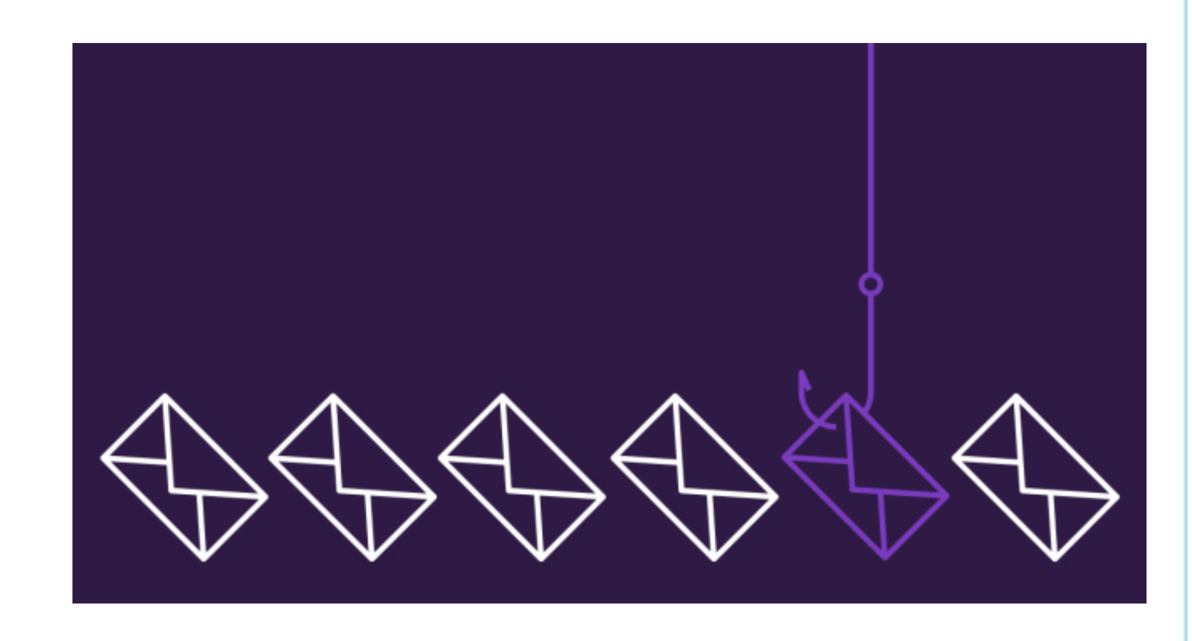


COMO CAPUTRAR TUS DATOS



Un anzuelo

- Eres mi competencia. ¿Me estás robando los datos?
- Después de ir acotando posibilidades, sí, eres tú!!
- Progresa adecuadamente

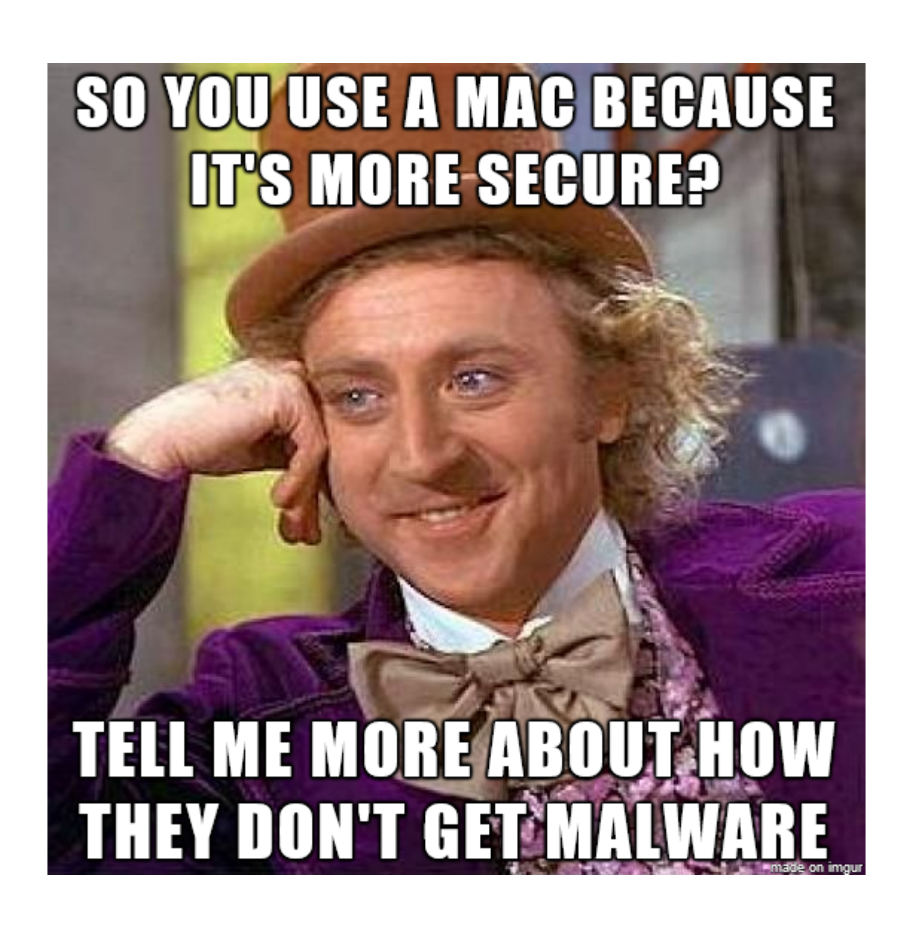




MITOS Y LEYENDAS



"Los Mac no tienen virus"



"El mito de que no hay virus para Mac es historia. Sólo en 2015 hemos detectado el doble de malware para estos sistemas que el que detectamos en 2014"

Luis Corrons, director de Panda Labs.



"Las compañías de antivirus hacen los virus"

¿Las compañías antivirus fabrican virus para tener un beneficio económico? ¿porque?

1 seguidor 6 respuestas

Respuestas Calificación

Mejor respuesta: Si lo hacen, lo hacen porque crean virus, que solo sus antivirus pueden detectar y eliminar, con eso venden mas su producto y ganan mas dinero.

Anónimo · hace 9 años

0 0 Comentario

porla misma razon de que Las Reliquias de la Muerte se divida en dos partes por mas dinero

OH FOR GOD'S SAKE

memegenerator.net

Mi respuesta favorita



"La ciberseguridad es un asunto exclusivo de TI"

No, no y mil veces no!!!

Pensar que las amenazas son algo que solo involucra al departamento de TI es una de las mejores maneras de que dichas amenazas tengan éxito.

Es importante recordar que la Ciberseguridad implica responsabilidades en la totalidad de los departamentos de toda la organización, desde sucursales como en centros de datos o dispositivos móviles.





EL ALCANCE DE LA PERICIAL





Forensic & Security

La profesión

WE DID IT!

Aunt Irma Visits



DUDAS?









Pilar.vila@forensic-security.com

@PilarinaVilla

Forensic & Security

